HELIXA PRIVACY POLICY

1.Introduction

This privacy policy ("**Privacy Policy**") has been implemented on behalf of Helixa Inc., Helixa SRL and the Telmar Group (the list of group entities is detailed below at Section 17, below) (collectively, referred to as "**Helixa**" or "**we**", "**us**" and "**our**"). It is designed to help you understand the personal data (as described in Section 2, below) we collect from you, why we collect it, what we do with it and how you can update, manage, export and delete your personal data. In the event your personal data is shared within the Telmar Group (Helixa Inc., and Helixa SRL are subsidiaries of Telmar Parent Corporation), this is done so in accordance with Sections 5 and 9 of this Privacy Policy. If you have any questions or concerns about our use of your personal data, please do not hesitate to contact us at the contact details set out in Section 15 of this Privacy Policy.

Quick Links

We recommend that you read this Privacy Policy in full to ensure you are fully informed. However, to make it easier for you to review those parts of this Privacy Policy which apply to you, we have divided up the document into the following Sections:

2. The Types of Personal Data that We Collect

Personal data is information that relates to an identified or identifiable individual, and it could be as simple as a name or a number, or could include other identifiers such as an IP address, a cookie identifier, or other factors.

We collect personal data in order to provide our services to you; maintain communications with you; and/or in order to comply with applicable law. Please note that if we have requested personal data from you and you decide that you do not want to share certain personal data with us, then this may prevent us from: (i) providing our services to you; or (ii) entering into a contract to provide services to you. In these circumstances we will ensure we notify you when reasonably possible to do so.

We collect different types of personal data for different reasons, including:

- **Customer Data:** customer user names, email addresses, business contact details and passwords, with whom we communicate in order to provide our services and/or for general business management purposes.
- **Support Data:** in order to provide support services to customers that subscribe to Helixa's services, we may process customer users' names and contact details to allow us to communicate and provide our support services to you.
- **Website Data:** when you visit our website (and certain other portals and third-party platforms), we or third parties may place certain cookies on your device related to the performance of these

websites and portals and analytics tools. For further details, please see our Websites & Cookies Notice.

- **Dataset Data:** As part of the services we provide to our customers we may receive and process data provided by third parties under separate license agreements. These datasets we receive may include data that may or may not be regarded as personal data in some jurisdictions, such as provider IDs, Public Twitter Handles, or other identifiers. If we receive such data, we will not generally make these data available to customers (unless they are the data controller of such data) and customers will only receive aggregated summaries that do not allow reverse engineering to identify any individuals. The exception to the foregoing may be in limited instances where customers may be able to see public "influencer" profiles/Twitter handles as a part of their search results.
- **Payment & Finance Data:** we may collect and process credit card and/or corporate bank account details that may contain personal data and information we receive from a customer that is used and processed for the sole purpose of receiving payments. Helixa uses a third-party service provider to manage credit card processing: Stripe. This service provider is not permitted to store, retain, or use information you provide except for the sole purpose of credit card processing on our behalf. You may review Stripe's privacy policy on their website (link: https://stripe.com/us/privacy).
- **Marketing Data:** in order to market to customers and potential customers, Helixa may collect and process names, contact details and marketing preferences in order to communicate with you.
- **Recruitment Data:** Helixa may also process personal data when you register for or apply for jobs either through third party recruitment agencies or portals or via Helixa's website. In that case, the personal data that Helixa may process may include information that you provide, such as your name, mailing address, e-mail address, telephone number, fax number, and background information required to apply for a job. You will receive a privacy notice upon receipt of your application to Helixa setting out further details of how your personal data may be used.
- **Biometric Data:** to the extent permitted by applicable law, either with your consent or by notice where you attend our offices, we may collect and process recordings of your voice and physical appearance obtained from recorded material collected via video conference or close circuit television (CCTV) that may identify you.

- Any other data that you voluntarily provide to us.

3. How do we obtain Your Personal Data

Most of the personal data we process about you is provided to us directly by you for one of the following reasons:

- when you contact us on our website;
- when you complete a registration form on our website;
- when you register for one of our webinars;
- when you attend a meeting or video conference, event or webinar that we host or attend;
- when you contact us via LinkedIn or Facebook;
- when you phone us;
- when you provide us with your details at an event;
- when you provide us with details in order to set up a contract for the provision of our services; and
- when you provide us with user details in order to set up user accounts to provide our services.

We may also receive personal data indirectly, from the following sources:

- from our dataset providers and data suppliers we partner with to provide our services. Although we do not specifically request personal data from such dataset and data providers, some of the data provided to us may in some cases and in some jurisdictions include personal data. Examples of this type of data includes but is not limited to IP addresses, User IDs, public Twitter handles, and geolocation information;
- from our third-party lead generation providers in order for us to send marketing material to individuals: (i) that have consented to their details being shared with us and to receive marketing material; or (ii) where we have a legitimate interest in sending you our marketing material and our legitimate interest does not override your data protection interests or your fundamental rights and freedoms; and
- from our third party partners in order for us to send marketing material to individuals: (i) that have consented to their details

being shared with us and to receive marketing material, or (ii) where we have a legitimate interest in sending you our marketing material and our legitimate interest does not override your data protection interests or your fundamental rights and freedoms.

We take reasonable measures to ensure that when we receive personal data indirectly: (i) the third party providing your personal data has the necessary lawful basis to share your personal data with us; and (ii) we use any such data in compliance with terms and conditions set out by the third party providing it to us.

4. Why do we Have Your Personal Data

We use your personal data in order to, where applicable:

- respond to any questions or requests;
- communicate with you and provide any further information about our services;
- maintain a business relationship with you, particularly where you subscribe to Helixa's services;
- undertake our contractual obligations to you, particularly where you subscribe to Helixa's services;
- provide our services to you;
- provide you with service support;
- manage any complaints or claims relating to services you provide to us, or our services we provide to you;
- include you in webinars;
- subject to applicable law and your marketing preferences, undertake direct marketing, advertising and public relations activities, in connection with Helixa and the Telmar Group's business activities, our packages and our services (including to make recommendations about our services, package updates, surveys, events and webinars), and to inform you about developments within Helixa and the Telmar Group;
- facilitate service improvement and development, to allow us to improve our packages and services or develop new packages and services for our customers;

- where necessary, comply with laws and regulations, under judicial authorisation, or to exercise or defend the legal rights of the Helixa group; and
- help us conduct our business more effectively and efficiently, or improve our packages and services.

In all circumstances, we only use your personal data for the purpose it was collected unless we reasonably believe that we need to use such personal data for another, related purpose, and it is legally possible to do so. If we need to use your personal data for any other purpose we will notify you and let you know the lawful basis on which we propose to rely.

5. Sharing Your Personal Data

We only share your personal data if it is necessary to do so in order to provide our services to you or enhance our relationship with you. Whenever we share your personal data with a third party provider we ensure that this is done so in accordance with applicable data protection laws by implementing appropriate measures to maintain the security and confidentiality of your personal data, and to ensure that your personal data is used in accordance with this Privacy Policy. We may share your personal data with the following categories of recipients:

- the Telmar Group, for details on the locations please see Section 17 below;
- third-party service providers that: (i) provide hosting services; (ii) provide data processing services; or (iii) process personal data for other purposes detailed in this Privacy Policy. These include but are not limited to:
    - IT service providers, for example Amazon Web Services and GSuite;
    - professional advisors, for example insurers, lawyers and other applicable professional bodies;
    - analytics and search engine providers that assist us, for the legitimate interest of improvement and optimisation of our products and services;
    - CRM service providers, for example Salesforce; and
    - marketing service providers;
- to any law enforcement body, regulatory, government agency, court or other third party where we believe disclosure is necessary, for example to exercise, establish or defend our legal rights, or we

are compelled to disclose such personal data to comply with the law;
- to a potential purchaser (and its agents and advisors) in connection with a proposed merger or acquisition of any part or all of our business, provided that the purchaser may not use your personal data for any purpose other than for the purposes detailed in this Privacy Policy; or
- to any other person you have consented to us to share personal data with.

In all circumstances that we share personal data with a third party we only do so to the extent that it is required for them to provide their services to us. At all times your personal data must be processed in accordance with (i) this Privacy Policy; and (ii) any additional data protection terms, incorporated into the agreement that we have with them, which are no less stringent than the protection afforded by this Privacy Policy.

6. Lawful Basis for Processing your Personal Data

Under the General Data Protection Regulation 2018 ("**GDPR**"), the lawful bases that we normally rely on for processing your personal data, detailed above, are:

- Consent. You are able to withdraw your consent at any time. You can do this by contacting privacy@telmar.com.
- Contractual Obligation. Where processing is necessary for the performance of our contractual obligations to you.
- Legitimate Interest. Where we have a legitimate interest in processing your personal data, if this is the case we will inform you of what our legitimate interest is at the time of collecting your personal data.

We may need to process your personal data in order to comply with applicable laws, in these circumstances we have a legal obligation to process your data, but we will inform you if this is the case.

In the unlikely event we store any Special Category Data (as defined by GDPR) the lawful basis for processing is determined by the category of

personal data being processed. In the event this relates to Special Category Data contained in a dataset, we rely on your consent to process such personal data.

Where we undertake direct marketing, all of our direct marketing campaigns are conducted in accordance with applicable law; we only do so with your consent and/or where we have a legitimate interest to do so, but in any event, you have the option to opt out of any direct marketing at any time by clicking the unsubscribe link in our marketing material. Helixa has performed a legitimate interests assessment in respect of its direct marketing activities to former, existing, and prospective customers. In summary, Helixa has a legitimate interest to market its services to existing customers as they already receive services directly from Helixa and may benefit from other services that Helixa provides. Former customers may be likely to purchase Helixa services after receiving marketing materials as they become aware of the additional benefits that other services could bring them. In addition, Helixa has a legitimate interest in marketing its services to prospective customers to promote brand awareness and increase sales.

To the extent that Helixa records any video conferences/calls/meetings of your voice or image (biometric data), Helixa will only do so with your explicit consent before such recordings are made.

7. How we Store Your Personal Data and for How Long

Helixa will retain your personal data only as long as necessary for the purposes for which it was collected; to provide you with services in accordance with our contractual obligations to you; and where required or permitted under law. Generally, this means your personal data will be retained until the end of your contractual relationship with us. In addition, such data may also be retained whilst Helixa has a legitimate business need to do so.

When we have no ongoing legitimate business need to process your personal data, we will either delete or anonymise it or, if this is not possible (for example, because your personal data has been stored in

backup archives), we will securely store your personal data and isolate it from any further processing until deletion is possible.

In relation to direct marketing, we will retain personal data (only to the extent necessary) in order to ensure we respect your direct marketing opt-out preferences.

8. Security

No service is completely secure, but we believe the security of your information is a serious issue and we are committed to maintaining commercially reasonable and appropriate security measures to ensure that your personal information is protected both online and offline. Helixa has a dedicated Information Security team that manages our framework, policies and procedures based on ISO27001 principles (with supplementary controls added for NIST framework alignment) to protect your personal information.

The framework includes (but not limited to) the following measures; employees and contractors being subject to background checks and bound by confidentiality, all receive training on data privacy and security. Those responsible for designing, managing and developing software and services do so applying secure development and privacy by design practices. Principles of least privilege are adopted using a role-based model for provisioning access to critical infrastructure and sensitive data. Data is encrypted in transit over public networks using both TLS, data encryption at rest is using Advanced Encryption Standard, pseudonymization. We also take measures to ensure third-party service providers that process personal data on our behalf also have appropriate security controls in place.

While we strive to protect your data, we cannot guarantee that unauthorized access to your data, data loss or a data breach will never occur.

9. International Data Transfers

In order to provide our services to you it may be necessary to transfer your personal data to a country that is different to the country in which we collected your personal data, and such country may not apply the same level of data protection.

As we are a global enterprise, and part of the Telmar Group, Helixa may transfer your personal data to Telmar Group companies (see section 17, below) and our third party services providers. To the extent required by applicable data protection law, any personal data that is transferred amongst Telmar Group companies shall be subject to an intra-group data transfer agreement ("**IGDTA**") that applies the Standard Contractual Clauses approved by the European Commission, and the UK's International Data Transfer Agreement and the International Data Transfer Addendum to the European Commission's Standard Contractual Clauses.

In addition to the IGDTA, Helixa performs transfer impact assessments (each a "**TIA**") in respect of the transfer of personal data outside the European Economic Area to "third countries". In this context, "third countries" are countries that the EU has not issued recognition of a country's adequacy of its data protection laws to ensure that a data subject gains a similar level of protection that a person would receive under GDPR. The purpose of a TIA is to evaluate whether the legislation in the third country might prevent the non-EU Data importer of personal data from complying with GDPR requirements – especially regarding potential data access rights of intelligence agencies. A TIA requires a diligent assessment of all circumstances of the transfer in question, the laws and practices of the third country of destination and any relevant contractual, technical or organizational safeguards put in place.

10. Additional Information for U.S. Residents in Certain States (Including California)

In addition to the data protection laws referred to in this Privacy Policy, we also comply with the relevant privacy laws in the United States, including, where applicable, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations ("**CCPA**"). The CCPA was implemented to enhance privacy rights and consumer protection for residents in

California and therefore it applies to businesses that carry our business activities in California.

Collection of Personal Information

When we act as a “Service Provider” (as defined in the CCPA) or a "Processor" (as defined in applicable US state privacy laws), we may process “Personal Information” or "Personal Data" on behalf of our customers or dataset providers. In such case, we will provide reasonable assistance to that customer or dataset provider as necessary to enable them to respond to your requests for the exercise of your privacy rights - you should therefore submit your request directly to the relevant customer or dataset provider.

"Personal Information" is defined as information as information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. We shall refer to such information as "**Personal Information**" throughout this Section.

In accordance with applicable US state privacy laws, Personal Information does not include:

- Publicly available information, such as government records or information that has lawfully been made available to the general public by the consumer or from widely distributed media; and
- De-identified or aggregated information.

Section 2 above (titled "The Types of Personal Data that We Collect") describes the types of Personal Information that we collect. We have collected within the last 12 months the following categories of Personal Information:

- Identifiers, such as your name, alias, postal address, email address, IP address or other similar identifiers;
- Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)), such as your contact information;
- Characteristics of protected classifications under California or federal law, such as your gender;
- Commercial information, such as transaction information;

- Internet or network activity information, such as your interactions with our website;
- Geolocation data, such as your approximate location based on your IP address;
- Audio, electronic, visual, and similar information, such as call or video recordings;
- Professional or employment-related information, such as your title or industry;
- Sensitive personal information as defined in the CPRA, such as your account log-in in combination with the password or credentials to access the account (if you have an account with us); and
- Inferences drawn from any of the above Personal Information to create a summary about you, for example of your preferences and characteristics.

We may use, process and disclose de-identified or aggregated and other non-identifiable information including related to our business and our services for quality control, analytics, research, development and other purposes. Such information will not identify you individually.

Where we use, disclose or process de-identified data (data that is no longer reasonably linked or linkable to an identified or identifiable natural person, household, or personal or household device) we will maintain and use the information in de-identified form and not to attempt to re-identify the information, except in order to determine whether our de-identification processes are reasonable and adequate pursuant to applicable privacy laws.

Sources of Personal Information

Section 3 above (titled "How do we obtain Your Personal Data") describes the sources of Personal Information that we collect.

Purposes of Processing Personal Information

Section 4 above (titled "Why do we Have Your Personal Data") describes the purposes of our use or processing of Personal Information.

Notwithstanding the purposes described above, we do not use or disclose of sensitive personal information beyond the purposes

authorized by applicable law (including the CCPA). Accordingly, we only use and disclose sensitive personal information as reasonably necessary (i) to perform our services requested by you, (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents, (iii) to detect, prevent and respond to malicious, fraudulent, deceptive, or illegal conduct, (iv) to verify or maintain the quality and safety of our services, (v) for compliance with our legal obligations, and (vi) to our service providers who perform services on our behalf.

Disclosure of Personal Information

Section 5 above (titled "Sharing Your Personal Data") describes the categories of recipients with whom we disclose Personal Information.

Certain US state privacy laws (such as the CCPA) define a "sale" as disclosing or making available to a third-party personal information in exchange for monetary or other valuable consideration, and also define “sharing” broadly, including as disclosing or making available personal information to a third party for purposes of cross-context behavioral advertising.

As mentioned above, we are in most cases a Service Provider or a Processor to a business that has provided your Personal Information to us for processing. Accordingly, we do not “sell” or “share” (as defined by applicable laws) such Personal Information to any third party.

Where we determine the purposes and means of the processing that we perform, for example when you provide the information directly to us or on our website, we are a "Business" (as defined in the CCPA) or a "Controller" (as defined in applicable US state privacy laws). In such case, we may disclose certain identifiers and Internet and electronic network activity usage information to advertising and data analytics partners and social networks. We may do so for the purposes described in Section 4 above (titled "Why do we Have Your Personal Data"), including (i) to provide, analyse and improve our website, products, and other services and (ii) develop and manage our relationships with you and our business partners.

In this circumstance, we rely on such laws' marketing exemption allowing us to: (i) store marketing information on third party systems, provided applicable terms are in place with our service provider; (ii)

provide opt-outs from marketing communications, as opposed to requiring an opt-in; and (iii) follow applicable cookie consents on our website.

We do not sell or share sensitive personal information, nor do we sell or share any Personal Information about individuals who we know are under sixteen (16) years old.

Do Not Track Browser Settings

California law requires us to let you know how we respond to web browser "Do Not Track" ("DNT") signals. Because there currently isn't an industry or legal standard for recognizing or honoring DNT signals, we do not respond to them at this time. For more information on DNT signals, visit http://www.allaboutdnt.com.

11. Information Pertaining to Children

Our website and our service are not intended for users under the age of 13, and we do not knowingly collect personal information relating to children, as defined by the U.S. Children's Online Privacy Protection Act ("COPPA") in a manner that is not permitted by COPPA. If a parent or guardian learns that a child has provided us with personal information, that child's parent or guardian should email us at privacy@telmar.com.

12. Your Data Protection Rights

When you subscribe to our services, you trust us with certain personal data. We understand that it is essential we work hard to protect your personal data and provide you with the access you need to feel in control of your personal data you provide to us.

In accordance with the applicable data protection laws in the European Union, you have the following rights with respect to your personal data, depending on the circumstances:

- your right of **access** - you have the right to ask us for copies of your personal data;
- your right to **rectification** - you have the right to ask us to rectify personal data you think is inaccurate. You also have the right to ask us to complete information you think is incomplete;
- your right to **erasure** - you have the right to ask us to erase your personal data in certain circumstances;
- your right to **restriction** of processing - you have the right to ask us to restrict the processing of your personal data in certain circumstances;
- your right to **object** to processing - you have the right to object to the processing of your personal data in certain circumstances;
- your right to data **portability** - you have the right to ask that we transfer your personal data you gave us to another organisation, or to you, in certain circumstances; and
- your right to lodge a complaint with **a supervisory authority.** We will use our best efforts to address and settle any requests or complaints brought to our attention. In addition, you have the right to approach the competent data protection authority with requests or complaints. This can be the supervisory authority in the country or federal state where you live.

You are not required to pay any charge for exercising your rights. If you do make a request, we will respond to you within one month. Please contact us by email at privacy@telmar.com.

13. Data Protection Rights for Residents in Certain U.S. States (including California)

Subject to certain limitations and exceptions under applicable law, verified residents in certain U.S. states (including California) may have, pursuant to applicable law, the following additional privacy rights with respect to their personal information:

- **Right to Know.** You have the right to ask us to disclose to you (i) the categories of personal information that we collect, (ii) the categories of sources from which the personal information is collected, (iii) the business or commercial purpose for collecting, selling, or sharing personal information, (iv) the categories of third parties to whom we disclose personal information, and (v) a copy

of the specific pieces of personal information we have collected about you.

- **Right to Access.** You have a right to ask us to provide you with a copy of the specific pieces of personal information that we retain about you.
- **Right to Correct.** Subject to certain conditions and exceptions, you have a right to request that we correct inaccurate personal information that we maintain about you, taking into account the nature and purposes of the processing of the personal information.
- **Right to Deletion.** You have the right to ask us to delete personal information we have collected about you, in certain circumstances.
- **Right to Limit Use and Disclosure.** Subject to certain conditions and exceptions, you have the right to limit the use and disclosure of sensitive personal information (as defined under applicable local laws). However, as stated above, we do not use or disclose your sensitive personal information for purposes except as described herein (and as permitted pursuant to applicable law, including where applicable, the CCPA).
- **Right to Non-Discrimination.** You have the right not to be subject to discriminatory treatment for exercising rights under the applicable privacy laws.
- **Right to Opt-Out.** Subject to applicable laws, you have the right to opt out of certain types of processing, including:
    - to opt out of the "sale" (as such term is defined under applicable law) of your personal information;
    - to opt out of targeted advertising by us (or for California residents, to opt out of the "sharing", as defined by the CCPA, of your personal information); and
    - to opt out of any processing of personal information for purposes of making decisions that produce legal or similarly significant effects.
- **Right to Appeal**. If we deny your privacy rights request, you may, depending on applicable law, also appeal our decision by submitting your appeal by contacting us at legal@helixa.com.

California's "Shine the Light" law (Civil Code Section § 1798.83) also permits California residents to request, once a year and free of charge, certain information regarding our disclosure of personal information to third parties for their direct marketing purposes in the preceding calendar year.

Please note that the rights described above are not absolute, and where an exception under applicable law applies, we may be entitled to refuse requests in whole or in part. You may exercise any of the above privacy rights by contacting us by email at privacy@telmar.com.

We will take steps to verify your request by matching the information provided by you with the information we have in our records. In particular, your request must:

- Provide sufficient information that allows us to reasonably verify you are the person about whom we collected personal information or an authorized representative.
- Describe your request with sufficient details that allows us to properly understand, evaluate, and respond to it.

Please note, in some cases, we may request additional information in order to verify your request or where necessary to process your request.

Authorized agents may initiate a request on behalf of another individual through one of the above methods; authorized agents will be required to provide proof of their authorization and we may also require that the relevant consumer directly verify their identity and the authority of the authorized agent.

14. Updates to this Privacy Policy

This Privacy Policy is current as of the date set forth below. Changes to this Policy will be posted on this website, along with information on any material changes. We reserve the right to update or modify this Privacy Policy at any time and without prior notice. Any modifications will apply only to the personal data we collect after the posting of the Privacy Policy. If we make material changes to how we collect, use and disclose the personal data we have previously collected about you, we will endeavor to provide you prior notice, such as by emailing you or posting prominent notice through on our website, and where required by applicable law provide you with the opportunity to opt out.

15. Our Contact Details

If you are unable to access this Privacy Policy due to a disability or any physical or mental impairment, please contact us and we will arrange to supply you with the information you need in an alternative format that you can access.

If you are resident in the European Economic Area or the United Kingdom our contact details are as follows:

Name:	Helixa SRL
Address:	via Arcivescovo Calabiana 6 Milano, 20139, Italy.
Addressee:	General Counsel
Email:	privacy@telmar.com

If you are resident anywhere other than the European Economic Area or the United Kingdom our contact details are as follows:

Name:	Helixa, Inc.
Address:	75 Varick Street - New York NY 10013
Addressee:	General Counsel
Phone Number:	+1 212 725 3000
Email:	privacy@telmar.com

16. How to Complain

If you have any concerns about our use of your personal data, you can make a complaint to us by email at privacy@telmar.com or at:
For the attention of: Legal Team,
Helixa,
Fora, 35-41 Folgate Street,
Spitalfields,
London,

E1 6BX

You can also complain to the ICO if you are unhappy with how we have used your personal data.

The ICO's address:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

17. Telmar Group Entities

We have set out below the Telmar Group Entities that we share personal data with in accordance with our intra-group data transfer agreement, further described in Section 9 above.

Helixa, Inc., a company incorporated in Delaware, with offices located at 75 Varick Street, 3rd Floor, New York, NY 10013.

Helixa SRL, a company incorporated in Italy, with offices located at via Arcivescovo Calabiana 6 Milano, 20139.

Telmar Group, Inc., a company incorporated in Delaware, with offices at 75 Varick Street, New York, NY 10013.

Telmar Information Services Corp., a company incorporated in New York, with offices at 75 Varick Street, New York, NY 10013.

Telmar HMS Limited, a company incorporated in Canada, with offices at 151 Yonge Street, Suite 1100, Toronto, Canada.

Telmar Europe Limited, a company incorporated in England and Wales, with offices at Fora, 35-41 Folgate Street, Spitalfields, London, E1 6BX.

Telmar Communications Limited, a company incorporated in England and Wales, with offices at Fora, 35-41 Folgate Street, Spitalfields, London, E1 6BX.

Telmar Peaktime SAS, a company incorporated in France, with offices at 15, place de la République, 3ème étage, 75003 Paris, France.

Telmar Peaktime B.V., a company incorporated in the Netherlands, with offices at Strawinskylaan 3051, 1077 ZX, in Amsterdam.

Telmar (Asia) Limited, a company incorporated in Hong Kong, with offices at Unit 46-106, 46/F, Lee Garden One, 33 Hysan Avenue, Causeway Bay, Hong Kong.

Telmar Software (Shanghai) Limited, a company incorporated in China, with offices at Unit Q-148, Room 501, 5/F, 700 Liyuan Road, Huangpu District, Shanghai, China.

Telmar Media Systems (Pty) Ltd, a company incorporated in South Africa, with offices at Building 26, 1st Floor, The Woodlands Office Park, Western Service Road, Woodmead, South Africa, 2196.

This Privacy Policy was updated on: 21 August 2023.